امن الحاسوب

هي عملية منع واكتشاف استعمال الحاسوب لاي شخص غير مسموح له وهي اجراءات تساعد على منع المستخدمين عير المسموح لهم بالدخول للحاسوب واستعمال ملفاته وان الكشف عن هذه العمليات تساعد في تحديد الشخص الذي حاول اقتحام النظام ونجح في ذلك وعن تصرفاته في الحاسوب .

الاختراق الالكتروني :

هو قيام شخص غير مخول او اكثر بمحاولة الوصول الكترونيا الى الحاسوب او الشبكة عن طريق شبكة الانترنت وذلك بغرض الاطلاع والسرقة التخريب والتعطيل باستخدام برامج متخصصة

انواع الاختراق الالكتروني

يمكن أن نقسم أنواع الاختراق من حيث الطريقة المستخدمة الى ثلاثة اقسام :

١- المزودات أو الأجهزة الرئيسية للشركات والمؤسسات او الجهات الحكومية وذلك بأختراق الجدران النارية التي توضع لحمايتها وغالبا يتم ذلك باستخدام المحاكاة Spoofing وهو مصطلح يطلق على عملية إنتحال شخصية للدخول الي النظام حيث أن حزم البيانات تحتوي على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة .

٢ - الأجهزة الشخصية والدخول عليها والعبث بما فيها من معلومات وتعد من الطرق الشائعة لقلة خبرة اغلب مستخدمي هذه الأجهزة من جانب ولسهولة تعلم برامج الأختراقات وتعددها من جانب اخر.

٣- البيانات من خلال التعرض والتعرف على البيانات اثناء انتقالها ومحاولة فتح التشفير إذا كانت البيانات مشفرة .وتستخدم هذة الطريقة تستخدم في كشف ارقام بطاقات الأئتمان وكشف الأرقام السرية للبطاقات البنوك

مصادر الاختراق الالكتروني :

١- مصادر متعمدة : ويكون مصدرها جهات خارجية تحاول الدخول الى الجهاز بصورة غير مشروعة بغرض قد يختلف حسب الجهاز المستهدف

ومن الامثلة عن المصادر المتعمدة للاختراق الالكتروني

- المحترفون والهواة لغرض التجسس دون الاضرار بالحاسوب
- اختراق شبكات الاتصال والاجهزة الخاصة بالاتصال للتنصت او للاتصال المجاني .
- اختراق لنشر برنامج معين او لكسر برنامج او لفك شفرتها المصدرية .
- اعداء خارجيون وجهات منافسة
- مجرمون محترفون في مجال الحاسوب والانترنت .

٢- مصادر غير معتمدة : وهي تنشئ بسبب ثغرات موجودة في برمجيات الحاسوب والتي قد تؤدي الى تعريض الجهاز الى نفس المشاكل التي تنتج عن الاخطار المتعمدة .

المخاطر الامنية الاكثر انتشارا :

١ – الفيروسات : هي برامج مصممة للانتقال الى اجهزة الحاسوب بطرق عدة وبدون اذن المستخدم وتؤدي الى تخريب او تعطيل عمل الحاسوب او اتلاف الملفات والبيانات

٢ – ملفات التجسس : وهي برامج مصممة لجمع المعلومات الشخصية مثل المواقع الالكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الالكترونية وكذلك تستطيع الحصول على امور مهمة للمستخدم مثل رقم بطاقة الائتمان دون علمه .

٣ – ملفات دعائية : وهي برامج مصممة للدعاية والاعلان وتغيير الاعدادت العامة في اجهزة الحاسوب مثل تغيير الصفحة الرئيسية للمتصفح واظهار بعض النوافذ الدعائية اثناء اتصالك بالانترنت وتصفحك للمواقع الالكترونية .

٤ – قلة الخبرة في التعامل مع بعض البرامج : مع ازدياد استخدام الانترنت من عامة الناس غير المتخصصين واستخدامهم وتعاملهم مع برامجيات متطورة الخاصة بخدمة تطبيقات الانترنت وبشكل مستمر وبدون خبرة كافية لكيفية التعامل مع تلك البرامجيات قد يفتح ثغرة في جهاز الحاسوب تمكن الاخرين من اختراق الجهاز .

٥ – اخطاء عامة : مثل سوء اختيار كلمة السر او كتابتها على ورقة مما يمكن الاخرين من قراءتها او ترك الحاسوب مفتوح مما يسمح للاخرين (خاصة غير المخولين او الغرباء) بالدخول لملفات الحاسوب او تغير بعض الاعدادات .

فايروسات الحاسوب :

هي برامج صغيرة خارجية صممت عمداً لتغيير خصائص الملفات التي تصيب وتقوم بتنفيذ بعض الاوامر اما بالحذف او التعديل او التخريب وفقا للاهداف المصممة لاجلها . ولها القدرة على التخفي ، ويتم خزنها داخل الحاسوب باحدى طرق الانتقال لالحاق الضرر به والسيطرة عليه .

الاضرار الناتجة عن فيروسات الحاسوب :

١ – تقليل مستوى الاداء الحاسوب

٢ – ايقاف تشغيل الحاسوب واعادة تشغيل نفسه تلقائيا كل بضع دقائق او اخفاقه في العمل بعد اعادة التشغيل .

٣ – تعذر الوصول الى مشغلات الاقراص الصلبة والمدمجة وظهور رسالة تعذر الحفظ لوحدات الخزن .

٤ – حذف الملفات او تغيير محتوياتها

٥ – ظهور مشاكل في التطبيقات المنصبة وتغير نوافذ التطبيقات والقوائم والبيانات

٦ – تكرار ظهور رسائل الخطأ في اكثر من تطبيق

٧ – افشاء معلومات واسرار شخصية هامة

صفات فايروسات الحاسوب :

١ – القدرة على التناسخ والانتشار

٢ – ربط نفسها ببرنامج اخر يسمى الحاضن (المضيف)

٣ – يمكن ان تنتقل من حاسوب مصاب لاخر سليم

أنواع الفيروسات

تقسم الفايروسات الى ثلاثة انواع

١ -**الفيروس** : برنامج تنفيذي (له امتداد (.com, .exe,.bat,.pif,.scrويعمل بشكل منفصل ويهدف إلى إحداث خلل في نظام الحاسوب. وتتروا خطورته حسب المهمه المصمم لاجلها فمنها البسيطة ومنها الخطيرة ، وينتقل بواسطة نسخ الملفات من جهاز به ملفات مصابة إلى جهاز آخر عن طريق الأقراص المدمجة سي دي وذاكرات الفلاش.

٢ -**الدودة** :تنتشر فقط عبر الشبكات والإنترنت مستفيدة من قائمة عناوين البريد الإلكتروني، مثل تطبيق برنامج التحدث الماسنجر فعند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في قائمة العناوين ويرسل نفسه إلى كل شخص في القائمة ، مما يؤدي إلى انتشاره بسرعة عبر الشبكة

٣ -**حصان طروادة :** فايروس تكون الية عمله مرفقا مع احد البرامج ، اي يكون جزءا من برنامج دون ان يعلم المستخدم . سمي هذا البرنامج بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونانيين داخله واستطاعوا اقتحام مدينة طرواده والتغلب على جيشها .

اهم الخطوات اللازمة للحماية من عمليات الاختراق :

الحفاظ على جهاز الحاسوب ضد هذه الملفات بشكل كامل صعب جدا مادام الجهاز مربوط بشبكة الانترنت ، ولكن يمكن حماية الحاسوب بنسبة كبيرة وتقليل خطر الاصابة بالاختراقات الالكترونية والبرامج الضارة باتباع الخطوات الاتية :

١- استخدام نظم تشغيل محمية من الفايروسات كنظم يونكس ولينكس ومشتقاتها .
٢ – تثبيت البرامج المضادة او المكافحة للفايروسات مثل (Norton , Kaspersky , Avira) وبرنامج مكافحة ملفات التجسس ذات الاصدارات الحديثة وتحديث النسخة .
٣ – الاحتفاظ بنسخ للبرمجيات المهمة مثل نظام التشغيل ويندوز وحزمة اوفيس ونسخة من ملفات المستخدم .
٤ – عدم فتح اي رسالة او ملف ملحق ببريد الكتروني وارد من شخص غير معروف للمستخدم او ملفات ذات امتدادات غير معروفة .
٥ – تثبيت كلمة سر Password على الحاسوب والشبكة اللاسلكية الخاصة بالمستخدم مع تغييرها كل فترة وعدم السماح الا للمستخدمين الموثوقين بالاتصال واستخدام الحاسوب .

٦ – عدم الاحتفاظ باية معلومات شخصية في داخل الحاسوب كـ (الرسائل الخاصة الصور ، الملفات المهمة والمعلومات المهمة مثل ارقام الحسابات او البطاقات الائتمانية) وخزنها في وسائط تخزين خارجية .

٧ – عدم تشغيل برمجيات الالعاب على نفس الحاسوب الذي يحتوي البيانات والبرامجيات المهمة لانها تعد من اكثر البرامجيات تداولا بين الاشخاص والتي تصاب بالفايروسات .

٨ – ايقاف خاصية مشاركة الملفات الا للضرورة وعمل نسخ احتياطية من الملفات المهمة والضرورية .

٩ – ثقافة المستخدم وذلك من خلال التعرف على الفايروسات وطرق انتشارها وكيفية الحماية منها ، والاثار المترتبة حال الاصابة بها . ويتم هذا عن طريق التواصل المستمر من خلال زيارة المواقع التي تهتم بالحماية من الفايروسات .

١٠ – فك الارتباط بين الحاسوب والموديم او الخط الهاتفي عند الانتهاء من العمل فذلك يمنع البرامج الخبيثة التي تحاول الاتصال من الدخول الى الحاسوب .

١١ – تفعيل عمل الجدار الناري .